

# Critical Information Protection: Focus on Detection



FBI Strategic Partnership Program

# Themes

- FBI in 2018
- Critical Information
- Security Posture
  - Prevent – Detect – Respond
- In Practice

# Assumptions

- Companies want to protect:
  - Users
  - PII
  - IP
  - Reputation
- There are hard and soft targets
- Governments use computer exploitation for collection or adversarial activity

# How Many Countries?

## Bloomberg

### **China's Sinovel Charged With Stealing Trade Secrets**

*Jun 27, 2013*

Sinovel Wind Group Co. , a Chinese wind-turbine company, was charged with stealing trade secrets from its former U.S. supplier, a case of industrial espionage that may heighten tensions in U.S.-China relations in the wake of the Edward Snowden affair.

U.S. prosecutors secured an indictment of the company and two of its executives in federal court yesterday in Madison, Wisconsin. Also charged was Dejan Karabasevic, who pleaded guilty in Klagenfurt, Austria, to stealing source code for the turbine controllers made by American Superconductor Corp. (AMSC), his former employer. The company lost more than \$1 billion in market value after the theft became public.

# FBI in 2018

- **Prosecute** or Don't
- **Tell us** or Don't
- We want to know about:
  - People trying to steal from you
  - Methods people use to steal
  - Actors and methods in other countries

# FBI Interests

- How information and secrets are taken
  - Methodologies
- Who is providing incentives
  - Where info is going
- What information is valuable
  - State-owned company, individual, or criminal group?
- How are companies working
  - Civil vs criminal
  - Legal vs HR vs security

# Two Paths

- Prosecution

- Individuals incentivized to steal
- Intent

- Intelligence

- Threats
- Actors
- Methods
- Targets

# Working with FBI

- Talk to us early
- If you've filed civil, criminal is probably not an option
  - Injunction is ok
- Our first questions:
  - What was taken
  - Who took it
  - How can you prove it
  - Did you protect it



# Critical Information

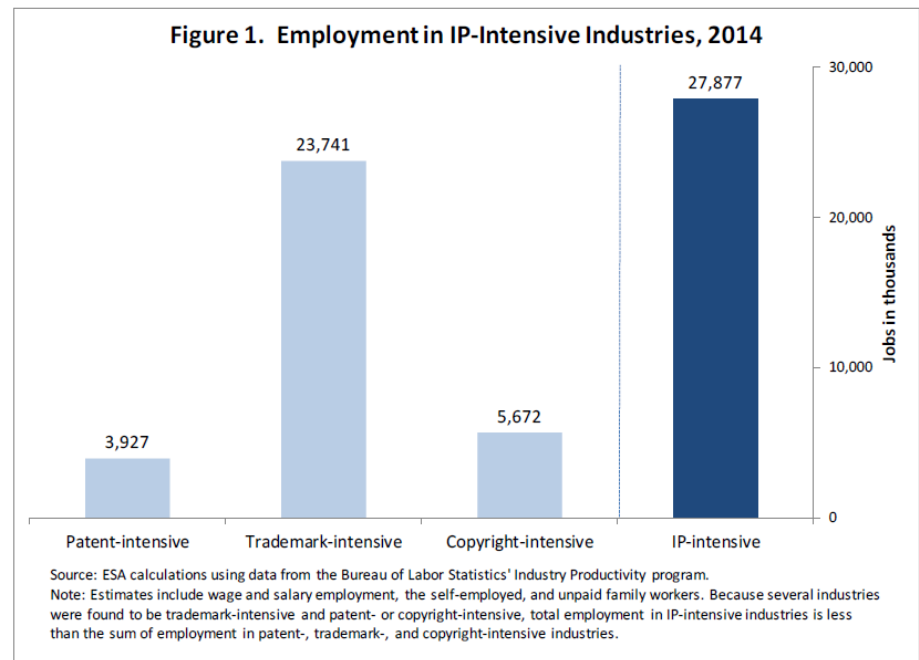
---

# It's an IP Economy

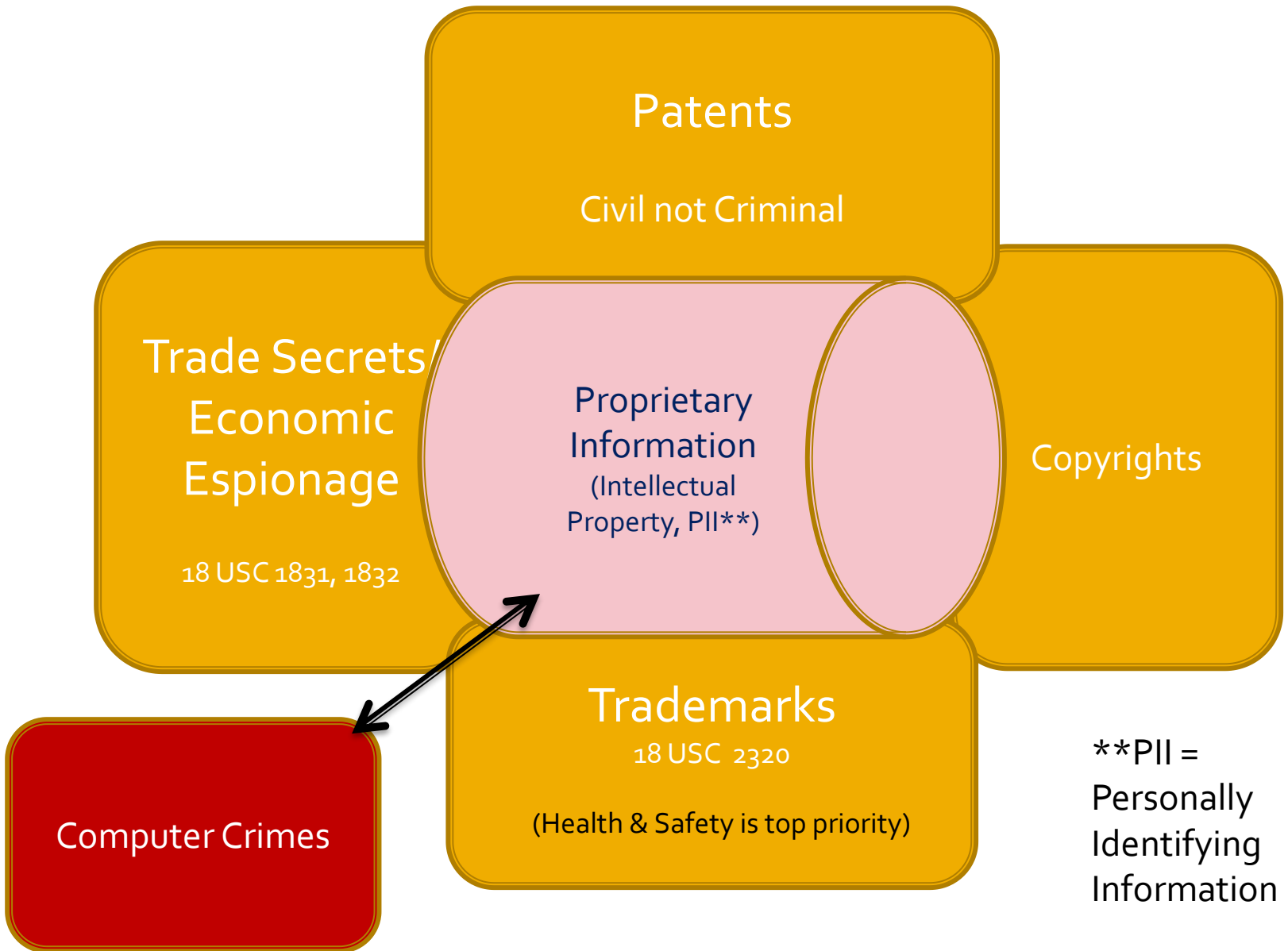
## [Intellectual Property and the U.S. Economy: 2016 Update | Department ...](#)

<https://www.commerce.gov/.../intellectual-property-and-us-economy-2016-update>

Sep 26, 2016 - Accordingly, the share of *total U.S. GDP* attributable to *IP-intensive industries* increased from 34.8 percent in 2010 to 38.2 percent in 2014. While *IP-intensive industries* directly accounted for 27.9 million *jobs* either on their payrolls or under contract in 2014, they also indirectly *supported* 17.6 million more



# Types of Critical Information



# Why Would You Be a Target?

- Access to sensitive industries
- Customer information
- Unethical competitors

# How Many Countries?

## Bloomberg

### **China's Sinovel Charged With Stealing Trade Secrets**

*Jun 27, 2013*

Sinovel Wind Group Co. , a Chinese wind-turbine company, was charged with stealing trade secrets from its former U.S. supplier, a case of industrial espionage that may heighten tensions in U.S.-China relations in the wake of the Edward Snowden affair.

U.S. prosecutors secured an indictment of the company and two of its executives in federal court yesterday in Madison, Wisconsin. Also charged was Dejan Karabasevic, who pleaded guilty in Klagenfurt, Austria, to stealing source code for the turbine controllers made by American Superconductor Corp. (AMSC), his former employer. The company lost more than \$1 billion in market value after the theft became public.

# Threat Assessment

Insiders, Hackers, Competitors, Criminals

---

# Security Posture

## Prevent – Detect – Respond Insider Threat

- Establish a baseline for key and high-risk employees
  - Joint effort between HR, IT, Security and Legal (e.g. Exit Interviews)
  - Annual assessment of key technologies or high profit products
- Provide managers with profile of security risk behaviors \*\*
  - What will you take action on?

## Information Technology

- What can you prove?
- Do you know where your secrets are? Are you maintaining reasonable measures for trade secret protection?

## Country/Competitor

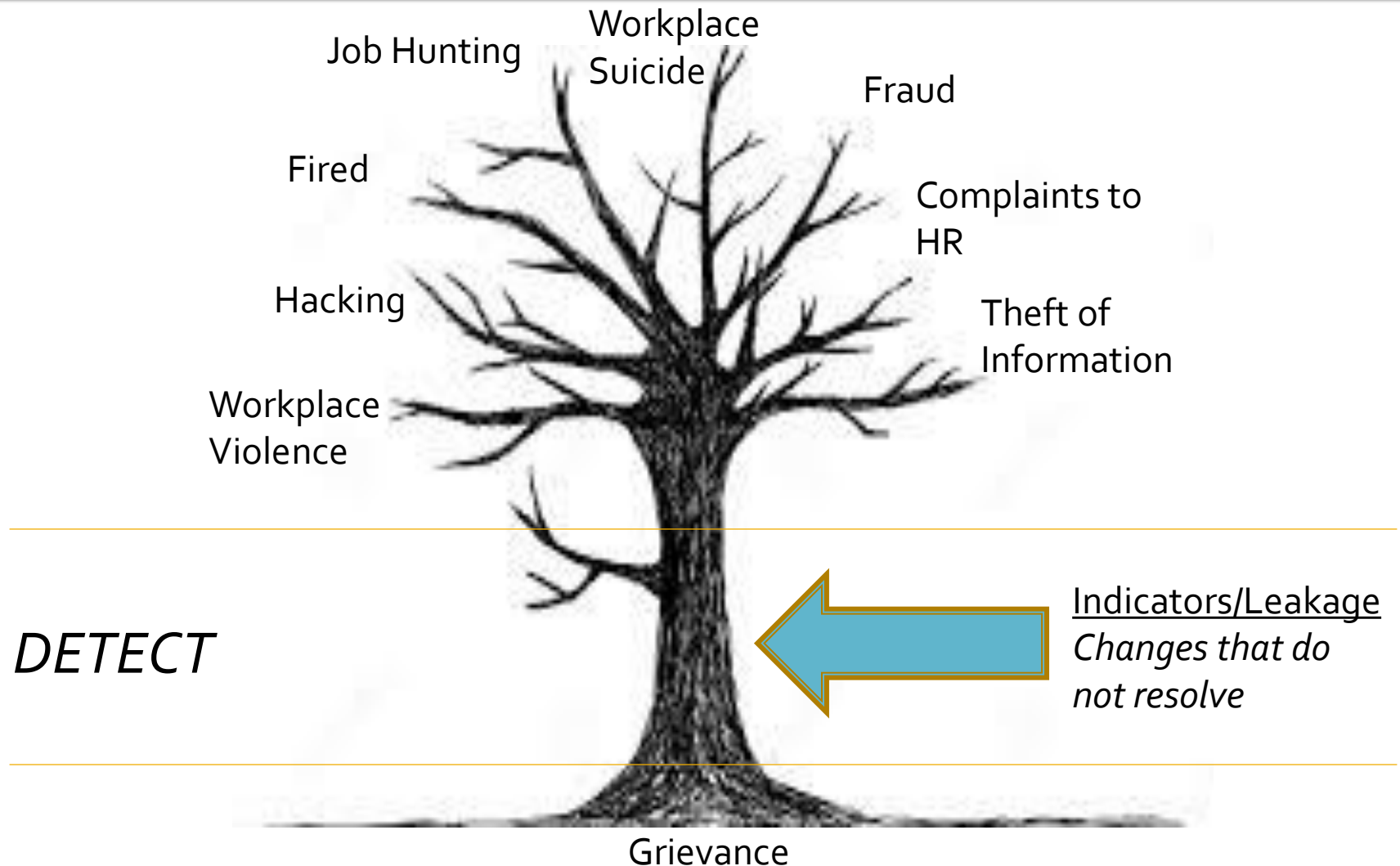
- Understand methods a country of competitor will use
- Ensure employees know what matters, what you will act on
- Assess risk of proprietary information in another country
- **Have a plan for when it gets stolen**

# Focus on Detection

- Prevent
  - Policies, training
- Detect
  - Delegated to HR, IT tools, or business managers
- Respond
  - Input from Legal, HR, IT, Business, Security



# Insiders: Detect Shared Warning Signs



# Behavioral Indicators

- Takes company information home via documents, thumb drives, disks, etc., without need or authorization
- Seeks information not related to their work duties, including information related to competitors or foreign entities
- Unnecessarily copies material
- Works odd hours without authorization; notable enthusiasm for overtime, weekend work, etc.
- Disregards company computer policies, to include installing personal software and downloading
- Remotely accesses network while on vacation, sick leave, or odd times
- Unreported foreign contacts or unreported overseas travel
- Short trips to foreign countries
- Unexplained affluence; living outside their means
- Overwhelmed by life crises or career disappointments
- Shows unusual interest in personal lives of co-workers
- Concern they are being investigated

[Return](#)

# Hacking as Espionage

CBS/AP / May 19, 2014, 8:25 AM

## U.S. files economic espionage charges against Chinese military hackers

*Last Updated May 19, 2014 5:00 PM EDT*

**WASHINGTON** - In a landmark case, the Department of Justice announced Monday charges against five Chinese military hackers, accusing them of stealing trade secrets and other proprietary or sensitive information online.

The hackers targeted big-name makers of nuclear and solar technology, stealing confidential business information, sensitive trade secrets and internal communications for competitive advantage, according to a grand jury indictment.



The DOJ specifically named "Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA)," as perpetrators in the

# Computer Exploitation: Methodologies

- ⦿ Spear-phishing email to targeted group
    - ⦿ Industry example
  - ⦿ Exploiting vulnerable machines
    - ⦿ Criminal or countries
    - ⦿ Missing patches
  - ⦿ Watering holes
- ⦿ All require an entry point into network

# Most Frequent & Successful

## **The Misplaced flash Drive**

One tried-and-true trick is “accidentally” dropping a flash drive in a company’s parking lot and hoping that a curious employee picks it up and plugs it into a company computer — thus launching the malware payload. While hardly new, this tactic is known to have a high rate of success.

## **Fake Windows Technical Support Calls**

The widely documented fake support calls from Windows Technical Support continue to defraud users. Essentially, scammers call their victims pretending to be from Microsoft to investigate a malware attack and try to persuade users to grant them remote desktop access. Once in, they pretend to discover a serious case of malware infestation—typically by installing scareware—and then proceed to extort a fee to resolve the problem.

# WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE



# Impersonation or Business Email Compromise

- A criminal impersonates you as an employee
- The impersonator contacts your customer via email
- Your customer pays the impersonator, thinking they were paying you
- ...or your customer clicks a link and gets hacked?

Your client/customer/boss would be...





# Case Examples

Insiders

---

# New Dog, Old Tricks

## Case Example #1

- Employee is fired
  - HR handles; security finds out as it happens
  - 5 years employment
  - No security flags
  - Signed trade-secret handling agreement
- In violation of policy, he is allowed to return to his desk
  - Security person escorts him
  - Observed putting disks & thumb drives in his bag

# New Dog, Old Tricks

## Case Example #1 (continued)

- IT review initiated
  - RESULT: Employee downloaded project information
  - Many previous downloads; unreviewed USB violations
- HR
  - RESULT: He was fired for failing to perform according to his employment agreement; failed to improve during performance plan
- Manager interview
  - RESULT: Employee applied to projects of interest and complained to his manager when he was denied

# New Dog, Old Tricks

## Case Example #1 (continued)

- Interview Co-Workers
  - RESULT: When he couldn't get approval to work on projects, he went to other employees and offered to "help you out"
  - Other employees unwittingly shared sensitive information
- FBI investigation continues successfully
- Discover employee is working at another company

# New Dog, Old Tricks

## Case Example #1- Part II

- Company #2
- You receive a call from the FBI
  - Inquiring about employee
  - How would your company detect if he was downloading trade secrets?
    - Assure FBI - System for detection is in place
    - Go Double-Check – is he downloading?
- You call FBI back
  - Detection measures failed
  - Employee has downloaded critical information

- On December 21, 2011, Kexue Huang was sentenced to 87 months in prison and three years of supervised release.

# Didn't See It Coming...

## Case Example #2

- IT Security notifies you
  - 12-year employee has downloaded critical information
- You ask IT for additional checks in email
- Check with HR
  
- A few days later...

# Didn't See It Coming

## Case Example #2 (continued)

- IT gives you a bunch of emails to review
  - You find:
    - e-mails to employee's personal e-mail
    - a business plan
    - itinerary for foreign travel
    - e-mails to another employee
- HR says there are no complaints
- You contact manager
  - Employee is a good performer
- Next Steps???



# Steps to Consider

- Review email
- Review internet browser history
- Attorneys who can say if information is trade secret
- Was it marked? Does it meet reasonable measures?

# My Bad Guy Lies Over the Ocean

- IT Security placed alarms on trade secret database
  - Employee Joon has downloaded 500+ formulas in a day
  - Employee Joon is in Asia; database is in MN
- Initial checks with management
  - They are moving a plant, appropriate to be moving formulas
- Second employee, Kim, triggers alarm
  - Same group, but he has been doing smaller amounts for over a month

# Over the Ocean (Continued)

- Check with manager
  - Employee Kim just gave his notice and left a week ago
  - Said he was working too hard
- Interview of Employee Joon
  - Kim asked me to copy all those formulas
  - Other employees – same story
- Next Steps?

# Decisions

- New Dog, Old Tricks
  - Much discussion then decided to prosecute
- Didn't See it Coming
  - Early discussions didn't show enough for prosecution
  - By second meeting, we knew there was enough; company decided to prosecute
- Over the Ocean
  - Company did not prosecute
  - Treated it entirely as a legal issue
    - Got employee to sign something, thought it was done

# In Practice

- Scenario 1:
  - Employee calls HR regarding a co-worker who was emailing chemical formulas to personal email account.
- If it went to thumb drive, can you prove it?

# In Practice

- Scenario 2:
  - Employee leaves to work for a competitor and took business development plans and strategic information.
- Was the information marked confidential? Do you have recourse?
- Would your employees do anything about it?



# Incident Handling - Intrusion

- Scenario 3:
  - Group of employees receives a very specific, personally-addressed email with a link. One person clicks the link.
- This is called spear-phishing. The link has put malware onto the computer. A government is now taking sensitive data from your network.
- You are surprised in a negotiation when you lose on all points.

# Economic Espionage Act of 1996

as amended

## ■ Theft of Trade Secrets, Title 18

- Section 1831
  - Punishes the theft of trade secrets to benefit  an government, instrumentality, or agent.
- Section 1832
  - Punishes the commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government.
- EEA protects against theft that occurs either:
  - in the United States **OR**
  -  outside the United States **AND**
    - an act in furtherance of the offense was committed in the United States, or
    - the violator is a US person or organization.
- Requires “Reasonable Measures” to protect trade secrets

[More](#)



# Takeaways

---

# Be Prepared

- Talk to FBI early
  - Keep my contact info
- Be ready to make decisions quickly
  - Threat Assessment Team
  - 10 days
- Other violations
  - Fraud
  - Embezzlement
  - Business Email Compromise

# Security Posture

## Prevent – Detect – Respond Insider Threat

- Establish a baseline for key and high-risk employees
  - Joint effort between HR, IT, Security and Legal (e.g. Exit Interviews)
  - Annual assessment of key technologies or high profit products
- Provide managers with profile of security risk behaviors \*\*
  - What will you take action on?

## Information Technology

- What can you prove?
- Do you know where your secrets are? Are you maintaining reasonable measures for trade secret protection?

## Country/Competitor

- Understand methods a country of competitor will use
- Ensure employees know what matters, what you will act on
- Assess risk of proprietary information in another country
- **Have a plan for when it gets stolen**

# For Your Family and Friends

- [ic3.gov](https://www.ic3.gov)
  - Reporting internet crime
  - 47 current scams
- Bad guys using phones more
  - Stuck somewhere – need money
  - Ransom



# Federal Bureau of Investigation Internet Crime Complaint Center(IC3)



[Home](#)   [File a Complaint](#)   [Press Room](#)   [News](#)   [About IC3](#)

## Internet Crime Prevention Tips

Internet crime schemes that steal millions of dollars each year from victims continue to plague the Internet through various methods. Following are preventative measures that will assist you in being informed prior to entering into transactions over the Internet:

[Auction Fraud](#)  
[Counterfeit Cashier's Check](#)  
[Credit Card Fraud](#)  
[Debt Elimination](#)  
[DHL/UPS](#)  
[Employment/Business Opportunities](#)  
[Escrow Services Fraud](#)  
[Identity Theft](#)  
[Internet Extortion](#)  
[Investment Fraud](#)  
[Lotteries](#)  
[Nigerian Letter or "419"](#)  
[Phishing/Spoofing](#)  
[Ponzi/Pyramid](#)  
[Reshipping](#)  
[Spam](#)  
[Third Party Receiver of Funds](#)

## Welcome to the IC3

## Site Navigation

[Alert Archive](#)  
[FAQs](#)  
[Disclaimer](#)  
[Privacy Notice](#)  
[Internet Crime Prevention Tips](#)  
[Internet Crime Schemes](#)

## Annual Report



2016 IC3 Annual Report

# Themes

- FBI in 2018
- Critical Information
- Security Posture
  - Prevent – Detect – Respond
- In Practice

# FBI Contact Information

- Minneapolis: Shena Crowe
  - [sbcrowe@fbi.gov](mailto:sbcrowe@fbi.gov)
  - 763-569-8487